Codes de Reed-Muller généralisés

Dany-Jack Mercier

IUFM de Guadeloupe, Morne Ferret,
BP399, Pointe-à-Pitre cedex 97159, France
dany-jack.mercier@univ-ag.fr

24 mai 2002

Résumé

Ce texte est une présentation concise des codes de Reed-Muller généralisés affines $\mathrm{GRM}(q, m, r)$ et projectifs $\mathrm{PRM}(q, m, r)$.

Soient m un entier naturel non nul, q une puissance d'un nombre premier, et $\mathbb{F}_q$ le corps fini à q éléments. On note $\mathcal{P} = \mathcal{P}(q, m) = \mathbb{F}_q[X_1, \ldots, X_m]$ l'algèbre des polynômes à m indéterminées à coefficients dans $\mathbb{F}_q$. On note aussi $X = (X_1, \ldots, X_m)$ et $\mathcal{P} = \mathbb{F}_q[X]$. Si $\alpha = (\alpha_1, \ldots, \alpha_m) \in \mathbb{N}^m$, on pose $X^\alpha = X_1^{\alpha_1} \ldots X_m^{\alpha_m}$. L'espace vectoriel des polynômes de de degré $\leq r$ sera noté indifféremment $\mathcal{P}_r$, $\mathcal{P}(q, m, r)$ ou $\mathbb{F}_q[X_1, \ldots, X_m]_r$. On pose enfin $\mathbb{N}_m = \{1, \ldots, m\}$.

1 Polynômes et fonctions polynomiales

Toute application $f : \mathbb{F}_q^m \to \mathbb{F}_q$ est polynomiale. En effet, si $a = (a_1, \ldots, a_m) \in \mathbb{F}_q^m$, le polynôme

$$e_a(X) = \prod_{i=1}^{m} (1 - (X_i - a_i)^{q-1})$$

vaut 1 si $X = a$, et 0 sinon. A partir de là, toute application f de $\mathbb{F}_q^m$ dans $\mathbb{F}_q$ s'écrit

$$f = \sum_{a \in \mathbb{F}_q^m} f(a) e_a$$

et le système $(e_a)_{a \in \mathbb{F}_q^m}$ engendre l'espace vectoriel $\mathcal{F}$ des applications de $\mathbb{F}_q^m$ dans $\mathbb{F}_q$. Comme ce système est libre, ce sera une base de $\mathcal{F} = \mathbb{F}_q^{\mathbb{F}_q^m}$. L'application

[0] [ccod0009] v1.01 http://perso.wanadoo.fr/megamaths

© 2002, D.-J. Mercier. Vous pouvez faire une copie de ces notes pour votre usage personnel.

$$\begin{array}{rlcl} c: & \mathcal{P} & - & \mathcal{F} \\ & P & - & (x - \quad P(x)) \end{array}$$

est un épimorphisme d'algèbres, et la donnée de c équivaut à celle de l'application

$$\begin{array}{rcl} \mathcal{P} & - & \mathbb{F}_q^{q^m} \\ P & - & \left(P\left(x^{(1)}\right) \quad P\left(x^{(q^m)}\right)\right) \end{array}$$

où $x^{(1)} \quad x^{(q^m)}$ représente une énumération de tous les éléments de $\mathbb{F}_q^{q^m}$. Cette seconde écriture de c revient à remplacer la fonction $c(P)$ par la q^m-liste de ses coordonnées dans la base $(e_a)_{a \quad \mathbb{F}_q^m}$.

Définition 1 *Le noyau $\mathcal{I} = \mathrm{Ker}\, c$ de c s'appelle l'**idéal des polynômes identiquement nuls** On le notera $\mathcal{I}(q \quad m)$ si une confusion est à craindre.*

Théorème 1 *L'idéal $\mathcal{I} = \mathrm{Ker}\, c$ est engendré par les polynômes $X_i^q - X_i$ ($i \quad \mathbb{N}_m$).*

Preuve : Montrons seulement l'inclusion non triviale $\mathrm{Ker}\, c \subset \mathcal{I}$. On raisonne par récurrence sur m. Si $m = 1$ et $P(x) = 0$ pour tout $x \quad \mathbb{F}_q$, par division euclidienne $P(X) = Q(X)(X^q - X) + R(X)$ avec $\deg R(X) < q$. Le polynôme R de degré $< q$ s'annulera en q valeurs distinctes, donc sera nul. Si l'inclusion est vraie jusqu'au rang $m-1$ et si $P \quad \mathrm{Ker}\, c$, par division euclidienne

$$\begin{aligned} P(X_1 \quad X_m) &= Q(X_1 \quad X_m)\ (X_m^q - X_m) + R_{q-1}(X_1 \quad X_{m-1})\, X_m^{q-1} + \\ &\qquad + R_0(X_1 \quad X_{m-1}) \end{aligned}$$

Pour tout $(x_1 \quad x_{m-1}) \quad \mathbb{F}_q^m$ fixé, le polynôme en X_m de degré $\leq q-1$

$$R_{q-1}(x_1 \quad x_{m-1})\, X_m^{q-1} + \quad + R_0(x_1 \quad x_{m-1})$$

admet q racines. Il est donc nul et $R_i(x_1 \quad x_{m-1}) = 0$ pour tout i. Cela étant vrai pour tout $(x_1 \quad x_{m-1}) \quad \mathbb{F}_q^{m-1}$, l'hypothèse récurrente appliquée aux polynômes R_i montre que $R_i \quad \mathcal{I}$ pour tout i. On déduit $P \quad \mathcal{I}$. ■

Définition 2 *On appelle **polynôme réduit** tout polynôme de $\mathcal{P}$ de degré $\leq q-1$ par rapport à chacune des variables, i.e. dont les seuls monômes sont $X_1^{\alpha_1} X_2^{\alpha_2} \quad X_m^{\alpha_m}$ avec $0 \leq \alpha_i \leq q-1$ pour tout i. Notons $\mathcal{R}$ (ou $\mathcal{R}(q \quad m)$) le sous-espace vectoriel de $\mathcal{P}$ formé par ces polynômes réduits.*

Théorème 2 *On a $\mathcal{P} = \mathcal{I} \oplus \mathcal{R}$. En particulier :*
1) $\mathcal{P} \ \mathcal{I} \quad \mathcal{R} \quad \mathcal{F}$,
2) chaque classe de $\mathcal{P} \ \mathcal{I}$ contient un seul polynôme réduit,
3) tout polynôme P s'écrit de façon unique sous la forme $P = Q + P^*$ où Q est identiquement nul et P^* est réduit.

Preuve : 1) Montrons que $\mathcal{P} = \mathcal{I} + \mathcal{R}$. Tout polynôme P de $\mathcal{P}$ est somme de monômes du type $aX_1^{\alpha_1} X_2^{\alpha_2} \quad X_m^{\alpha_m}$ et il suffit de montrer que chacun de ces monômes se décompose dans $\mathcal{I} + \mathcal{R}$ pour conclure. Montrons donc que tout monôme $P = X_1^{\alpha_1} X_2^{\alpha_2} \quad X_m^{\alpha_m}$ s'écrit $P = Q + P^*$ avec $Q \quad \mathcal{I}$ et $P^* \quad \mathcal{R}$. Procédons par récurrence sur $n = \mathrm{Sup}\,(\alpha_1 \quad \alpha_m)$. Si $n \leq q-1$, le monôme P est déjà réduit et la décomposition est triviale. Si la décomposition existe pour tout monôme $X_1^{\alpha_1} X_2^{\alpha_2} \quad X_m^{\alpha_m}$ tel que $\mathrm{Sup}\,(\alpha_1 \quad \alpha_m) \leq n$ avec $n \geq q - 1$, montrons qu'elle existe pour les monômes $X_1^{\alpha_1} X_2^{\alpha_2} \quad X_m^{\alpha_m}$ tels que $\mathrm{Sup}\,(\alpha_1 \quad \alpha_m) = n+1$. Il existe $j \quad \mathbb{N}_m$ tel que $\alpha_j = n + 1 \geq q$. Pour tout $x_j \quad \mathbb{F}_q$, $x_j^{\alpha_j} = x_j^{\alpha_j - q} x_j^q = x_j^{\alpha_j - q+1}$ donc

$$X_1^{\alpha_1} \quad X_j^{\alpha_j} \quad X_m^{\alpha_m} - X_1^{\alpha_1} \quad X_j^{\alpha_j - q+1} \quad X_m^{\alpha_m} \quad \mathcal{I} \qquad\qquad (*)$$

L'hypothèse récurrente montre que $X_1^{\alpha_1} \quad X_j^{\alpha_j - q+1} \quad X_m^{\alpha_m} \quad \mathcal{I}+\mathcal{R}$, de sorte que $(*)$ entraîne $P \quad \mathcal{I} + \mathcal{R}$.

2) Montrons que $\mathcal{I} \quad \mathcal{R} = \quad 0$ par récurrence sur le nombre de variables m. Si $m = 1$, un polynôme $P(X_1) = \sum_{j=0}^{q-1} a_j X_1^j$ de $\mathcal{I} \quad \mathcal{R}$ sera nécessairement nul puisque de degré $\leq q - 1$ et admettant q racines. Au rang m, supposons que le polynôme $P \quad \mathbb{F}_q\,[X_1 \quad X_m]$ appartienne à $\mathcal{I} \quad \mathcal{R}$. Ecrivons

$$P\,(X_1 \quad X_m) = A_{q-1}\,(X_1 \quad X_{m-1})\, X_m^{q-1} + \quad + A_0\,(X_1 \quad X_{m-1})$$

où chacun des polynômes $A_0 \quad A_{q-1} \quad \mathbb{F}_q\,[X_1 \quad X_{m-1}]$ est réduit.
Pour tout $(x_1 \quad x_{m-1}) \quad \mathbb{F}_q^{m-1}$ fixé, le polynôme

$$P\,(x_1 \quad x_{m-1} \; X_m) = A_{q-1}\,(x_1 \quad x_{m-1})\, X_m^{q-1} + \quad + A_0\,(x_1 \quad x_{m-1})$$

en X_m est de degré $\leq q-1$ et admet q racines, c'est donc le polynôme nul. Par conséquent $A_j\,(x_1 \quad x_{m-1}) = 0$ pour tout j et pour tout $x_1 \quad x_{m-1}$ dans $\mathbb{F}_q$, et l'on peut écrire $A_j \quad \mathcal{I} \quad \mathcal{R}$. L'hypothèse récurrente entraîne maintenant $A_j = 0$ pour tout j, soit $P = 0$. ■

Théorème 3 $\dim \mathcal{P}_r = C_{m+r}^m$.

Preuve : On dénombre les monômes du type $X_1^{\alpha_1} X_2^{\alpha_2} \quad X_m^{\alpha_m}$ où $\sum_{i=1}^{m} \alpha_i \leq r$, ceux-ci formant une base de $\mathcal{P}_r$.

1) Première solution : Combien y-a-t'il de m-listes $(\alpha_1 \quad \alpha_m) \quad \mathbb{N}^m$ vérifiant l'équation $\alpha_1 + \quad + \alpha_m = t$? A chaque m-listes solution on associe un tableau formé d'une ligne sur laquelle on place $m - 1$ cloisons délimitant m emplacements. On place α_1 boules dans le premier emplacement, α_2 boules dans le second, etc jusqu'à épuisement des t boules. Il y a autant de solutions que de tableaux et autant de tableaux que de façons de choisir les places de $m - 1$ cloisons parmi $m - 1 + t$ places possibles, soit C_{m-1+t}^{m-1}. Le nombre de solutions entières de $\alpha_1 + \quad + \alpha_m \leq r$ sera donc $\sum_{t=0}^{r} C_{m-1+t}^{m-1} = C_{m+r}^m$.

2) Deuxième solution : On cherche le cardinal $A\,(m \; r)$ (resp. $B\,(m \; r)$) de l'ensemble des fonctions $f : \mathbb{N}_m - \quad 0 \quad r$ telles que $\sum_{x \quad \mathbb{N}_m} f(x) \leq r$ (resp. $\sum_{x \quad \mathbb{N}_m} f(x) = r$). On a

$$\begin{cases} A\,(m \; r) = A\,(m \; r - 1) + B\,(m \; r) \\ A\,(m - 1 \; r) = B\,(m \; r) \end{cases}$$

d'où $A\,(m \; r) = A\,(m \; r - 1) + A\,(m - 1 \; r)$. Il suffit alors de vérifier par récurrence que $A\,(m \; r) = C_{m+r}^m$. ■

2 Code de Reed-Muller affine $\mathrm{GRM}\,(q\ \ m\ \ r)$

Définition 3 *Le* ***code de Reed-Muller généralisé*** $\mathrm{GRM}\,(q\ \ m\ \ r)$ *d'ordre* r *est l'image de l'application*

$$\begin{array}{rccc} c: & \mathcal{P}_r & - & \mathcal{F} \\ & P & - & (x - \quad P(x)) \end{array}$$

ou, ce qui revient au même, de l'application évaluation

$$\begin{array}{rccc} c: & \mathcal{P}_r & - & \mathbb{F}_q^{q^m} \\ & P & - & (P\,(x))_{x \quad \mathbb{F}_q^m} \end{array}$$

On note $\mathrm{GRM}\,(q\ \ m\ \ r) = \mathrm{Im}\, c$*.*

La longueur du code $\mathrm{GRM}\,(q\ \ m\ \ r)$ est q^m.

• Si $r < q$, $\mathcal{P}_r \subset \mathcal{R}$ et l'application c est injective. Dans ce cas

$$\dim \mathrm{GRM}\,(q\ \ m\ \ r) = \dim \mathcal{P}_r = C_{m+r}^r$$

• Si $r \geq m(q-1)$, l'ensemble des polynômes réduits est inclus dans $\mathcal{P}_r$ et l'application c est surjective. Ici $\mathrm{GRM}\,(q\ \ m\ \ r) = \mathbb{F}_q^{q^m}$ n'offre plus d'intérêt.

• Si $q \leq r < m(q-1)$, l'application c est ni injective, ni surjective. Notons $\mathcal{R}_r$ l'espace vectoriel des polynômes réduits appartenant à $\mathcal{P}_r = \mathbb{F}_q\,[X_1 \qquad X_m]_r$. On a l'égalité $\mathcal{R}_r = \mathcal{P}_r \quad \mathcal{R} = R\,(\mathcal{P}_r)$ où $R : \mathcal{P} \qquad \mathcal{R}$ désigne la projection sur $\mathcal{R}$ parallèlement à $\mathcal{I}$. Dans ce cas la restriction

$$\begin{array}{rccc} c_{\ \mathcal{R}_r}: & \mathcal{R}_r & - & \mathbb{F}_q^{q^m} \\ & P & - & (P\,(x))_{x \quad \mathbb{F}_q^m} \end{array}$$

de c à $\mathcal{R}_r$ est injective et son image est le code de Reed-Muller $\mathrm{GRM}\,(q\ \ m\ \ r)$. Un article paru vers 1969 nous donne la dimension de $\mathcal{R}_r$ (que nous admettrons ici) :

$$\dim \mathrm{GRM}\,(q\ \ m\ \ r) = \dim \mathcal{R}_r = \sum_{t=0}^{r} \sum_{j=0}^{m} (-1)^j\, C_m^j C_{t-jq+m-1}^{t-jq}$$

On peut donc énoncer :

Théorème 4 *La dimension de* $\mathrm{GRM}\,(q\ \ m\ \ r)$ *est*

$$\dim \mathrm{GRM}\,(q\ \ m\ \ r) = \begin{cases} C_{m+r}^r & \text{si } r < q, \\ \sum_{t=0}^{r} \sum_{j=0}^{m} (-1)^j\, C_m^j C_{t-jq+m-1}^{t-jq} & \text{si } q \leq r < m(q-1), \\ q^m & \text{si } m(q-1) \leq r \end{cases}$$

Remarque : Calculons $\dim \mathcal{R}_r$ lorsque $r = q$. L'application

$$R_{\ \mathcal{P}_r} : \mathcal{P}_r \qquad \mathcal{R}_r$$

est surjective et $\dim \mathcal{P}_r = C_{m+r}^r$. Si $(e_1 \quad e_s)$ est une base de $\mathcal{P}_r$, tout revient à trouver le rang de $R(e_1) \quad R(e_s)$. Classons les éléments $X_1^{\alpha_1} X_2^{\alpha_2} \quad X_m^{\alpha_m}$ où $\ _{i=1}^{m} \alpha_i \leq r$ de la base de $\mathcal{P}_r$ en 2 parties A et B. A est formé des monômes tels que tous les α_i sont $< q$. Ces monômes resteront linéairement indépendants dans $\mathcal{R}_r$. Dans B mettons tous les monômes dont l'un des α_i vaut q. On obtient les monômes X_1^q, X_2^q, $\ $, X_m^q qui, une fois réduits, s'écrivent $X_1 \ X_2 \quad X_m$ et sont déjà comptés dans A. Finalement, le rang de $R(e_1) \quad R(e_s)$ sera $C_{m+r}^r - m$. ■

Théorème 5 *Si $r < q$ la distance minimale du code* $\mathrm{GRM}\,(q \ m \ r)$ *est*

$$\mathrm{dist}\,(\mathrm{GRM}\,(q \ m \ r)) = (q - r)\, q^{m-1}$$

Preuve : Le nombre maximum de racines dans $\mathbb{F}_q^m$ d'un polynôme quelconque de degré r de $\mathbb{F}_q\,[X_1 \quad X_m]$ est rq^{m-1} ([7] Th. 6.13 p. 275). ■

De façon plus générale :

Théorème 6 *{[3] Th. 5 p. 192} Si $0 < r < m\,(q-1)$, la distance minimale du code* $\mathrm{GRM}\,(q \ m \ r)$ *est $d = (q-b)q^{m-a-1}$ où $r = (q-1)a + b$ et $0 \leq b < q - 1$.*

Corollaire 1 *Si d désigne la distance minimale du code* $\mathrm{GRM}\,(q \ m \ r)$*, il existe au moins un polynôme réduit ayant $q^m - d$ racines dans $\mathbb{F}_q^m$. De plus, tout polynôme réduit de $\mathbb{F}_q^m\,[X_1 \quad X_m]$ possédant strictement plus de $q^m - d$ racines dans $\mathbb{F}_q^m$ sera identiquement nul.*

Idée de prolongement : Recommencer cette construction avec les polynômes homogènes ou les polynômes de permutation.

3 Code de Reed-Muller projectif $\mathrm{PRM}\,(q \ m \ r)$

3.1 Définition

L'espace projectif $\mathbb{P}^m\,(\mathbb{F}_q)$ de dimension m sur $\mathbb{F}_q$ est un ensemble fini de cardinal

$$\pi_m = 1 + q + \quad + q^{m-1} + q^m = \frac{q^{m+1} - 1}{q - 1}$$

Soit $\mathcal{H}(q \ m+1 \ r)$ le sous-espace de $\mathcal{P}(q \ m+1 \ r)$ formé des polynômes homogènes de degré r. Chaque polynôme homogène f de $\mathcal{H}(q \ m+1 \ r)$ permet de définir la fonction

$$\begin{array}{llcl} T_r\,(f): & \mathbb{P}^m\,(\mathbb{F}_q) & - & \mathbb{F}_q \\ & (x_0 : x_1 : \quad : x_m) & - & T_r(f)\,(x_0 \ x_1 \quad x_m) \end{array}$$

en posant

$$T_r(f)(x_0 : \cdots : x_{k(x)} : 0 : \cdots : 0) = \frac{1}{x_{k(x)}^r} f(x_0 \ \cdots \ x_{k(x)} \ 0 \ \cdots \ 0)$$

Dans cette écriture, $(x_0 : x_1 : \quad : x_m)$ désigne la $(m+1)$-liste des coordonnées homogènes d'un point de $\mathbb{P}_m(\mathbb{F}_q)$, et l'on a posé $k(x) = \mathrm{Max}\ j \quad x_j = 0$. On définit ainsi une application linéaire

$$\begin{array}{rccc} T_r : & \mathcal{H}(q\ \ m+1\ \ r) & - & \mathbb{F}_q^{\mathbb{P}^m(\mathbb{F}_q)} \\ & f & - & T_r(f) \end{array}$$

de noyau $\mathrm{Ker}\, T_r = \mathcal{I}_r$ où $\mathcal{I}_r = \mathcal{H}(q\ \ m+1\ \ r) \quad \mathcal{I}$ désigne le sous-espace vectoriel des polynômes identiquement nuls et homogènes de degré r.

Définition 4 *Le* ***code de Reed-Muller projectif*** $\mathrm{PRM}(q\ \ m\ \ r)$ *est par définition l'image de l'application* T_r*. On note* $\mathrm{PRM}(q\ \ m\ \ r) = \mathrm{Im}\, T_r$*.*

La longueur du code $\mathrm{PRM}(q\ \ m\ \ r)$ est π_m, et il suffit de choisir une énumération de $\mathbb{F}_q^{\mathbb{P}^m(\mathbb{F}_q)}$ pour obtenir les mots de code dans $\mathbb{F}_q^{\pi_m}$.

3.2 Dimension de $\mathrm{PRM}(q\ \ m\ \ r)$

On sait que $\dim(\mathcal{H}(q\ \ m+1\ \ r)) = C_{m+r}^r$ et

$$\dim(\mathrm{PRM}(q\ \ m\ \ r)) = \dim(\mathcal{H}(q\ \ m+1\ \ r)) - \dim \mathrm{Ker}\, T_r \qquad (\ )$$

La dimension de $\mathcal{I}_r = \mathrm{Ker}\, T_r$ nous est donnée par les deux Théorèmes suivants :

Théorème 7 *([8] Th. 2.1) L'espace vectoriel* $\mathcal{I}_r$ *des polynômes homogènes de degré* r *dans* $\mathcal{P}(q\ \ m+1\ \ r)$ *et identiquement nuls est décrit par les polynômes* f *tels que*

$$f(X_0\ \ X_1\ \cdots\ \ X_m) = \quad_{0 \le i < j \le m} (X_i^q X_j - X_i X_j^q) Q_{i\,j}(X_0\ \ X_1\ \cdots\ \ X_m)$$

avec $Q_{i\,j} \quad \mathcal{H}(q\ \ m+1\ \ r-q-1)$ *si* $r \ge q+1$*, et* $Q_{i\,j} = 0$ *si* $r \le q$*. Autrement dit* $\mathcal{I}_r$ *coïncide avec la* r*-ième composante homogène* $\mathcal{J}_r$ *de l'idéal* $\mathcal{J}$ *de* $\mathcal{P}(q\ \ m+1\ \ r)$ *engendré par les polynômes* $X_i^q X_j - X_i X_j^q$*, où* $0 \le i\ \ j \le m$*.*

Théorème 8 *([8] Th. 5.2) La dimension de la composante homogène* $\mathcal{J}_r$ *de degré* r *de l'idéal homogène* $\mathcal{J}$ *engendré par les polynômes* $X_i X_j^q - X_i^q X_j$ *est*

$$\dim \mathcal{J}_r = \quad_{j=2}^{m+1} (-1)^j C_{m+1}^j \quad_{\alpha=0}^{j-2} C_{r+(\alpha+1)(q-1)-jq+m}^m$$

La formule ( ) devient :

Théorème 9

$$\dim \mathrm{PRM}(q\ \ m\ \ r) = C_{m+r}^r - \quad_{j=2}^{m+1} (-1)^j C_{m+1}^j \quad_{\alpha=0}^{j-2} C_{r+(\alpha+1)(q-1)-jq+m}^m$$

L'article de Sorensen [9] propose une autre formule combinatoire :

Théorème 10

$$\dim \mathrm{PRM}\,(q\ \ m\ \ r) = \sum_{\substack{t=d\ \ mod\ \ q-1 \\ 0<t\le d}} \ \sum_{j=0}^{m+1} (-1)^j C_{m+1}^{j} C_{t-jq+m}^{m}$$

où le coefficient binômial C_{t-jq+m}^{m} *est nul si* $t - jq < 0$.

References

[1] Delsarte P., Goethals J.M. & Mac Williams F.J., "On Generalized Reed-Muller Codes and their Relatives", Inform. and Control 16, pp403-442, 1970.

[2] Kasami T., Lin S. & Peterson W.W., "Some results on cyclic codes which are invariant under the affine group, Scientific Report, AFCRL-66-622, Air Force Cambridge Research Labs., Bedford, Massachusetts, 1966.

[3] Kasami T., Lin S. & Peterson W.W., "New Generalization of the Reed-Muller Codes-Part I : Primitives Codes", IEEE Trans. Information Theory IT-14, pp.189-199, 1968.

[4] Kasami T., Lin S. & Peterson W.W., "Polynomial codes", IEEE Trans. Information Theory IT-14, pp.807-814, 1968.

[5] Lachaud G., "The parameters of Projective Reed-Muller Codes", Discrete Mathematics 81 pp217-221, 1990.

[6] Lachaud G., "Number of points of plane sections and linear codes defined by forms on algebraic varieties", Arithmetic, Geometry and Coding Theory, R. Pellikan, M. Perret and S.G. Vladut editors, Walter de Gruyter, pp77-104, 1996.

[7] Lidl, R., Niederreiter, H., "Finite Fields", Encyclopedia of Mathematics and its applications, vol. 20, Cambridge University Press, Cambridge, 1983.

[8] Mercier D-J. & Rolland R., "Polynômes homogènes qui s'annulent sur l'espace projectif $\mathbb{P}^m(\mathbb{F}_q)$", Journal of Pure and Applied Algebra 124, pp227-240, 1998.

[9] Sørensen A.B., "Projective Reed-Muller Codes", IEEE Trans. Inform. Theory 37, 1991.